GF(2 K) Elliptic Curve Cryptographic Processor Architecture Based N Bit Level Pipelined Digit Serial Multiplication

Gutub, A.A.-A.; Dept. of Comput. Eng., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia;

Computer Systems and Applications, 2003. Book of Abstracts. ACS/IEEE International conference;Publication Date: 14-18 July 2003;ISBN: 0-7803-7983-7
King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

Summary form only given. New processor architecture for elliptic curve encryption is proposed. The architecture exploits projective coordinates to convert GF(2 k) division needed in elliptic point operations into several multiplication steps. The processor has three GF(2 k) multipliers implemented using bit-level pipelined digit serial computation. It is shown that this results in a faster operation than using fully parallel multipliers with the added advantage of requiring less area. The proposed architecture is a serious contender for implementing data security systems based on elliptic curve cryptography.